Gaggle Safety Management User Guide / Additional Resources

Setting Up SSO with Okta

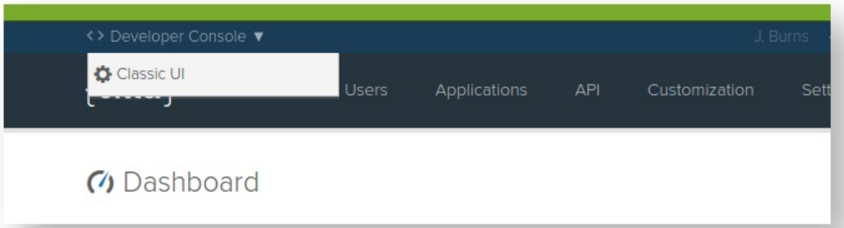
Created by Corey Tutewiler
Last updated Mar 21, 2019 by Jerad Burns

This documentation outlines setting up SSO with Okta acting as the IDP and Gaggle as the SP.

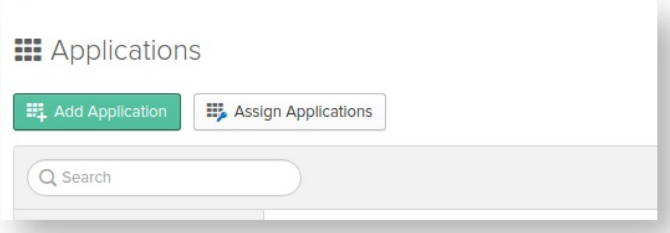
For Authority3 customers, please substitute https://apps.authority3.com in place of https://apps.gaggle.net.

Gaggle Logo for App Setup

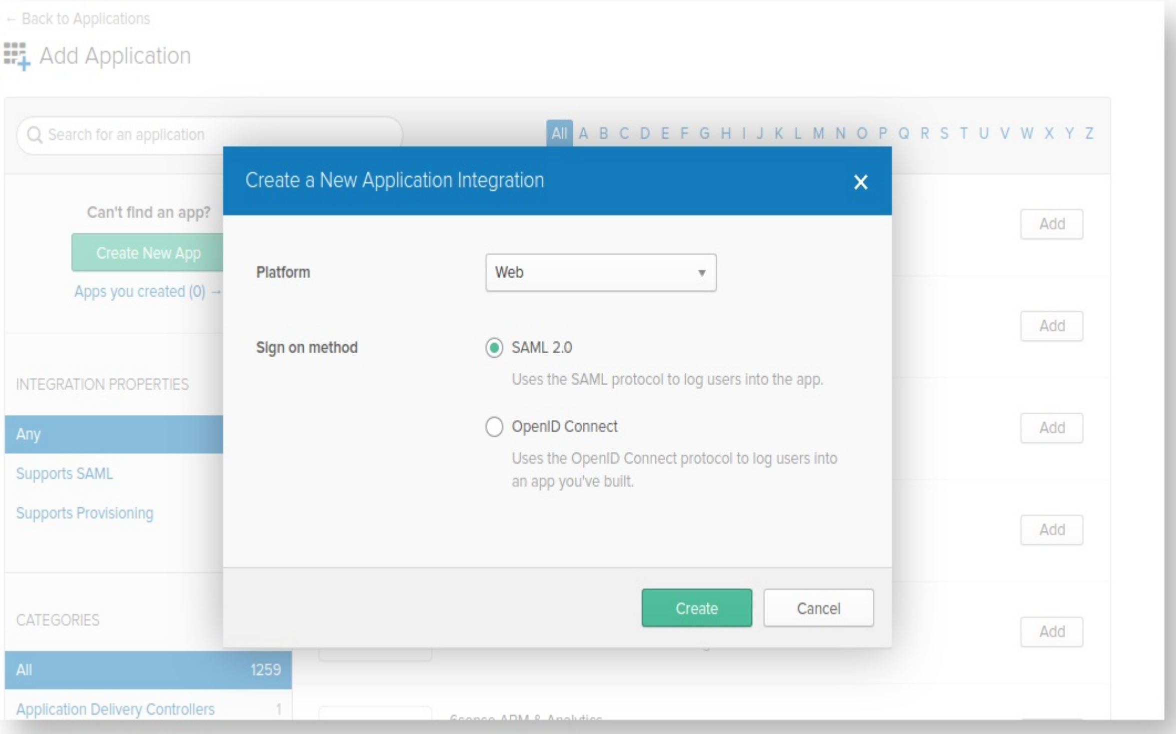
1. Log into Okta dashboard and switch to the 'Classic UI'.



2. From the main menu select 'Applications'
3. Click the 'Add Application' button



4. Click the 'Create New App' button
5. Set the Platform field to 'Web' and Sign on method to SAML 2.0



← Back to Applications

Add Application

Search for an application

All A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Can't find an app?

Create New App

Apps you created (0) →

INTEGRATION PROPERTIES

Any

Supports SAML

Supports Provisioning

CATEGORIES

All 1259

Application Delivery Controllers 1

Add

Create a New Application Integration ×

Platform: Web ▾

Sign on method

● SAML 2.0

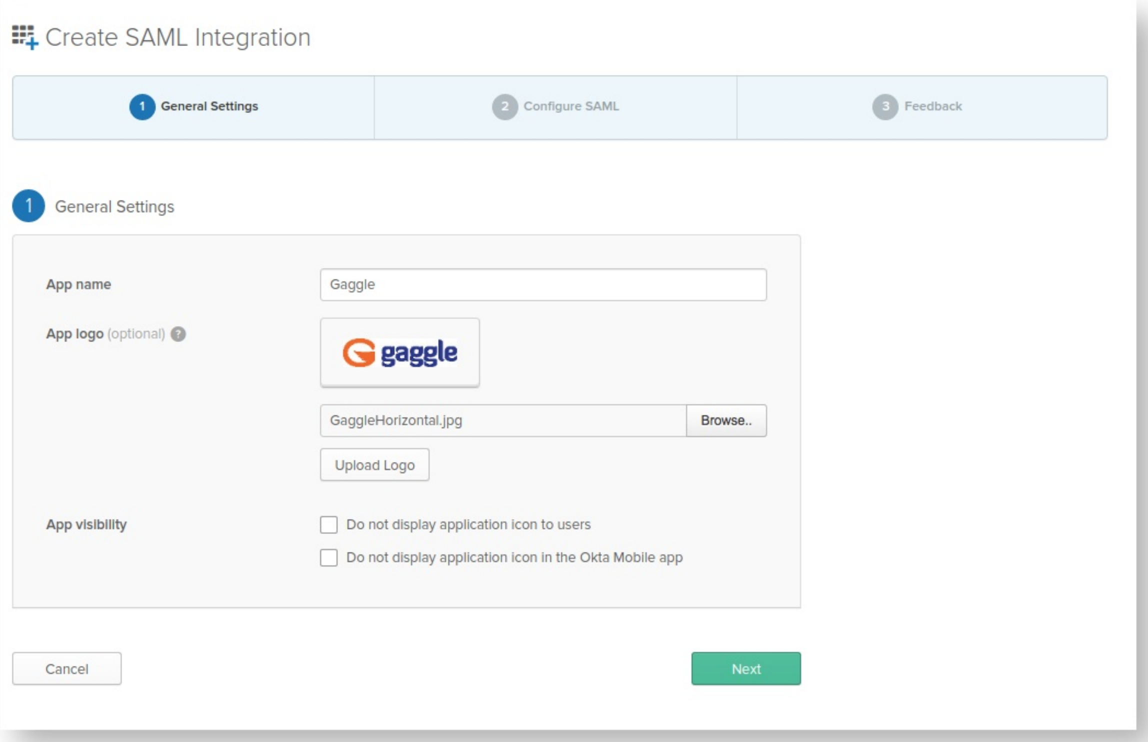
Uses the SAML protocol to log users into the app.

○ OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

Create Cancel

6. Set App Name to Gaggle and upload JPG for the App Logo and click Next



Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: Gaggle

App logo (optional) ?

GaggleHorizontal.jpg Browse..

Upload Logo

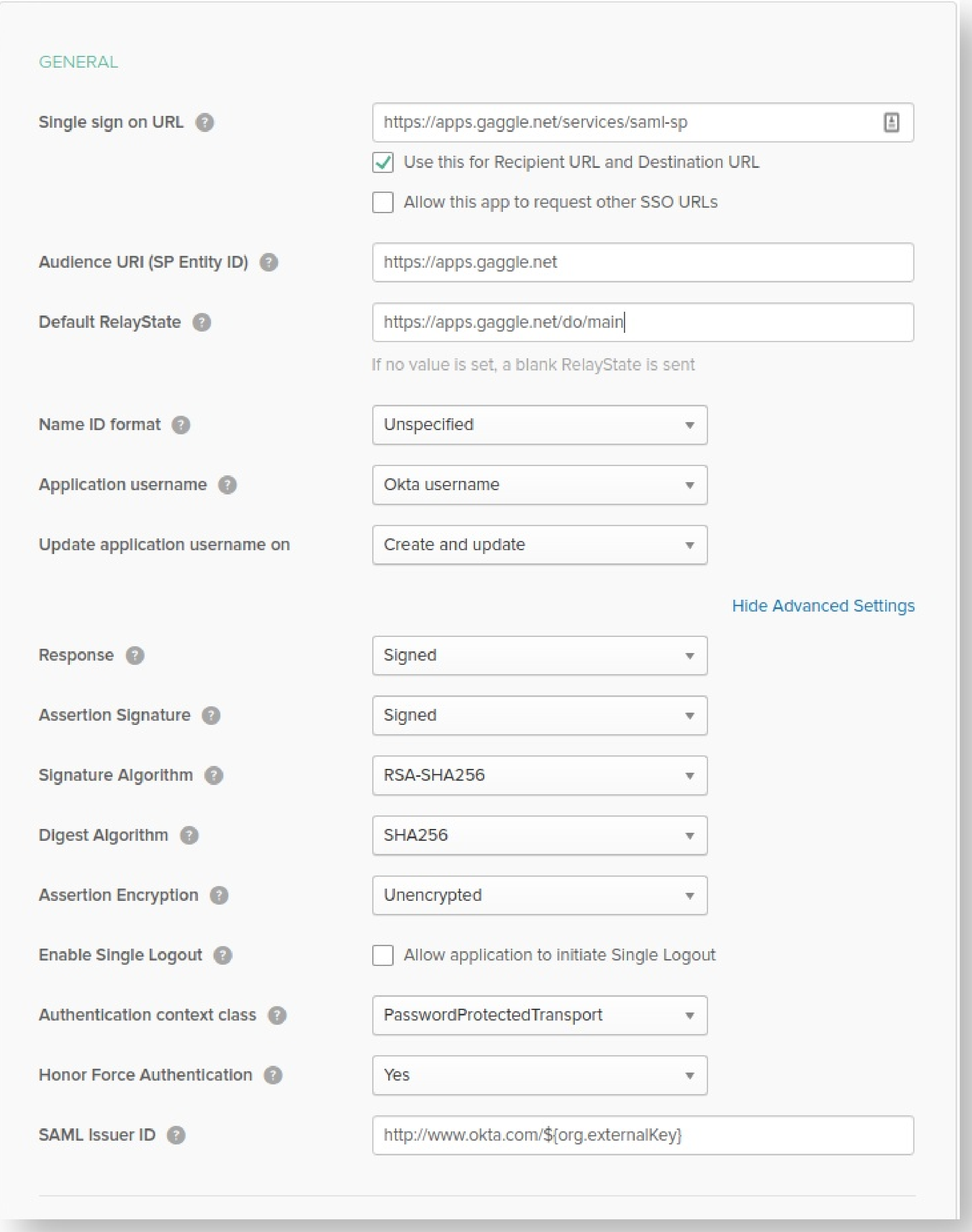
App visibility

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile app

Cancel Next

7. Under SAML Settings



GENERAL

Single sign on URL	https://apps.gaggle.net/services/saml-sp ☑ Use this for Recipient URL and Destination URL ☐ Allow this app to request other SSO URLs
Audience URI (SP Entity ID)	https://apps.gaggle.net
Default RelayState	https://apps.gaggle.net/do/main If no value is set, a blank RelayState is sent
Name ID format	Unspecified
Application username	Okta username
Update application username on	Create and update

Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	☐ Allow application to initiate Single Logout
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/${org.externalKey}

a. Single sign on URL
    i. https://apps.gaggle.net/services/saml-sp

b. Audience URI
    i. https://apps.gaggle.net

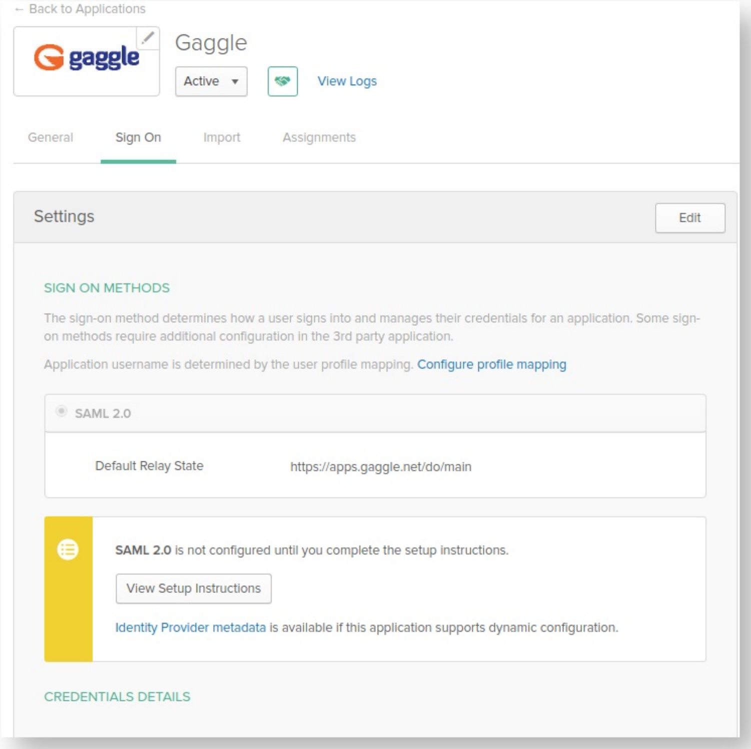
c. Default RelayState
    i. https://apps.gaggle.net/do/main

d. SAML Issuer ID
    i. http://www.okta.com/${org.externalKey}

e. Leave all other settings at their default value

8. Click Next
9. Click the radio button for "I'm an Okta customer adding an internal app"

10. Click the checkbox for "This is an internal app that we have created"
11. Click Finish
12. On the resulting page, in the Settings pane click 'View Setup Instructions'



SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State https://apps.gaggle.net/do/main

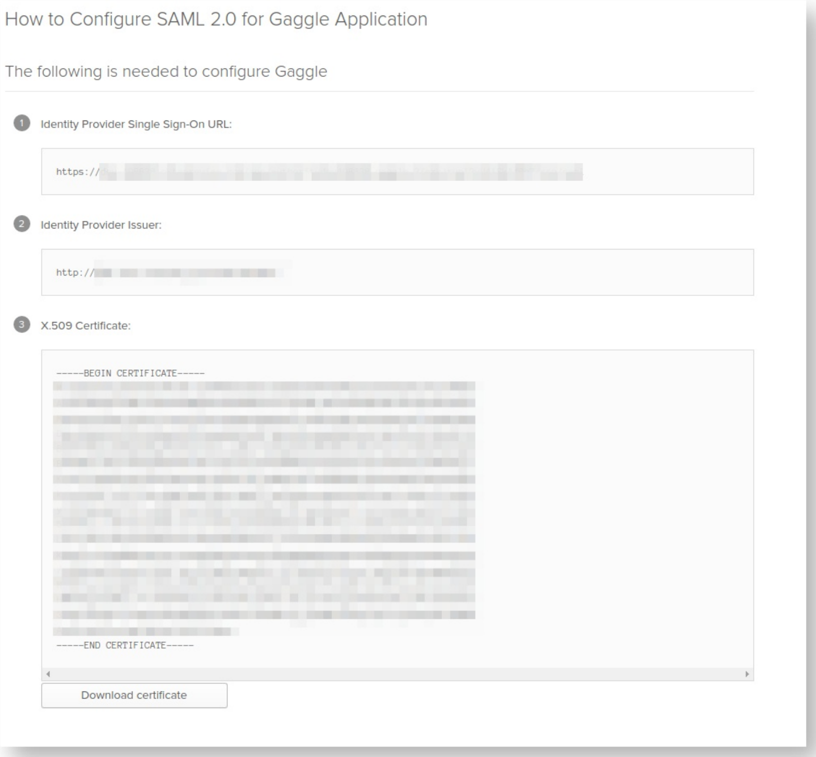
SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

CREDENTIALS DETAILS

13. Send the "Identity Provider Single Sign-On URL", "Identity Provider Issuer", and "X.509 Certificate" to Gaggle Support.



How to Configure SAML 2.0 for Gaggle Application

The following is needed to configure Gaggle

1 Identity Provider Single Sign-On URL:

```
https://[redacted]
```

2 Identity Provider Issuer:

```
http://[redacted]
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
```

okta sso